JOURNAL OF NUMBER THEORY 8, 224–232 (1976)

Positive Definite Rational Functions of Two Variables Which Are Not the Sum of Three Squares

M. R. CHRISTIE

Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge, England

Communicated by J. W. S. Cassels

Received June 22, 1973

Cassels, Ellison, and Pfister have shown that there is a positive semidefinite function of $\mathbf{R}(x, y)$ that is not the sum of three squares. In this paper positive definite functions of $\mathbf{R}(x, y)$ are found having the same property. The proof involves showing the nonexistence of points on some elliptic curves defined over $\mathbf{C}(x)$, and extends the methods of [1].

Pfister showed in [4] that every positive semidefinite function in $\mathbf{R}(x_1, \ldots, x_n)$ is a sum of 2^n squares of functions in $\mathbf{R}(x_1, \ldots, x_n)$. In general it is not known whether there are either positive definite or positive semidefinite functions of n variables that are not the sum of fewer than 2^n squares. Cassels, Ellison, and Pfister [1] have shown that there is a positive semidefinite function of two variables that is not the sum of three squares of elements of $\mathbf{R}(x, y)$; namely, $1 + x^4y^2 + y^4x^2 - 3x^2y^2$. In this paper we find strictly positive definite functions in $\mathbf{R}(x, y)$ that are not the sum of three squares in $\mathbf{R}(x, y)$; for example $(1 + 250xy^2)^2 + x(x + 3)^3 y^2$.

As in [1], the proof involves determining the points defined over $\mathbf{C}(x)$ on an elliptic curve $Y^2 = X(X - a + 2b)(X - a - 2b)$, where a, b are in $\mathbf{Q}(x)$. The points defined over $\mathbf{C}(x)$ are all defined over $K(x)$ where K is some normal algebraic number field. The Galois group of $K/\mathbf{Q}$ acts on the group of $K(x)$ points and we use this action to show that if our curve has points of infinite order over $\mathbf{C}(x)$, then one of an infinite set of other elliptic curves has points over $k(x)$, where k is a fixed algebraic number field. Then by choosing the initial curve carefully we ensure that each of the infinite set of curves has no points in some completion of $k(x)$.

1. PRELIMINARIES

Proposition 1 is proved in [1] and restated here for convenience. The results concerning isogenies are from the general theory of elliptic curves.

Let $F(x, y) = 1 + ay^2 + b^2y^4$ where $a, b \in \mathbf{Q}[x]$. F is positive definite if for each $t \in \mathbf{R}$ $1 + a(t)\,z + b^2(t)\,z^2 = 0$ has complex or negative roots, that is either

$$a^2(t) - 4b^2(t) < 0 \text{ or } a(t) \geqslant 0, \qquad \text{for each } t \in \mathbf{R}.$$

PROPOSITION 1. *Suppose a and b satisfy the above conditions. Then F is the sum of three squares in $\mathbf{R}(x, y)$ if, and only if, there is a point (α, β) defined over $\mathbf{R}(x)$ on the curve $\mathscr{C}^{-1}$: $-Y^2 = X(X^2 - 2aX + a^2 - 4b^2)$ with α and $-(\alpha^2 - 2a\alpha + a^2 - 4b^2)$ both positive semidefinite. Call such points of $\mathscr{C}^{-1}$ "special."*

For each $d \in \mathbf{C}^*$ let $\mathscr{C}^d$ be the curve $dY^2 = X(X^2 - 2aX + a^2 - 4b^2)$ and $\mathscr{D}^d$ be the curve $dY^2 = X(X^2 + 4aX + 16b^2)$, and abbreviate $\mathscr{C}^1$ to $\mathscr{C}$. Denote the points at infinity by $\mathfrak{o}$ and $\mathfrak{o}'$, respectively. $\mathscr{C}^d$ has three points of order two $\mathfrak{p}_0 = (0, 0)$, $\mathfrak{p}_+ = (a + 2b, 0)$, $\mathfrak{p}_- = (a - 2b, 0)$. For any field K, extending $\mathbf{Q}(x)$, let $\mathscr{C}_K{}^d$, $\mathscr{D}_K{}^d$ be the group of points on $\mathscr{C}^d$, $\mathscr{D}^d$, respectively, defined over K.

There are isogenies $\theta_1 : \mathscr{D}^d \to \mathscr{C}^d$, $\theta_2 : \mathscr{C}^d \to \mathscr{D}^d$, given by

$$\theta_1(\alpha, \beta) = \left(\frac{d\beta^2}{4\alpha^2}, \frac{(\alpha^2 - 16b^2)\,\beta}{8\alpha^2}\right), \qquad \text{if } \alpha \neq 0,\ \theta_1(0, 0) = \theta_1(\mathfrak{o}') = \mathfrak{o},$$

$$\theta_2(\alpha, \beta) = \left(\frac{d\beta^2}{\alpha^2}, \frac{(\alpha^2 - a^2 + 4b^2)\,\beta}{\alpha^2}\right), \qquad \text{if } \alpha \neq 0,\ \theta_2(\mathfrak{p}_0) = \theta_2(\mathfrak{o}) = \mathfrak{o}'.$$

The $\theta_1\theta_2$ and $\theta_2\theta_1$ are multiplication by 2 on $\mathscr{C}^d$ and $\mathscr{D}^d$, respectively. The images $\theta_1(\mathscr{D}_K{}^d)$ and $\theta_2(\mathscr{C}_K{}^d)$ are the kernels of maps $\varphi_1 : \mathscr{C}_K{}^d \to K^*/K^{*2}$ and $\varphi_2 : \mathscr{D}_K{}^d \to K^*/K^{*2}$; respectively, where

$$\varphi_1(\alpha, \beta) = d\alpha K^{*2}, \qquad \text{if } \alpha \neq 0,$$
$$\varphi_1(\mathfrak{p}_0) = (a^2 - 4b^2)\,K^{*2}, \qquad \varphi_1(\mathfrak{o}) = K^{*2},$$

and

$$\varphi_2(\alpha, \beta) = d\alpha K^{*2}, \qquad \text{if } \alpha \neq 0,$$
$$\varphi_2(0, 0) = \varphi_2(\mathfrak{o}') = K^{*2}.$$

Define $\varphi_3 : \mathscr{C}_K{}^d \to (K^*/K^{*2})^3$ by

$$\varphi_3(\alpha, \beta) = (\alpha d K^{*2}, (\alpha - a + 2b)\,dK^{*2}, (\alpha - a - 2b)\,dK^{*2}), \qquad \text{if } \beta \neq 0,$$
$$\varphi_3(\mathfrak{p}_0) = ((a^2 - 4b^2)\,K^{*2}, (-a + 2b)\,dK^{*2}, (-a - 2b)\,dK^{*2}),$$
$$\varphi_3(\mathfrak{p}_+) = ((a + 2b)\,dK^{*2}, 4bdK^{*2}, 4b(a + 2b)\,K^{*2}),$$
$$\varphi_3(\mathfrak{p}_-) = ((a - 2b)\,dK^{*2}, -4b(a + 2b)\,K^{*2}, -4bdK^{*2}),$$
$$\varphi_3(\mathfrak{o}) = (K^{*2}, K^{*2}, K^{*2}).$$

Then φ_3 is a homomorphism with kernel $2\mathscr{C}_K{}^d$.

LEMMA 1. *Let k be a field extension of $\mathbf{Q}$ in which b and $a^2 - 4b^2$ split into linear factors. Take $K = \mathbf{C}(x)$ and $d = 1$. Then representatives for the image of φ_3 can be chosen in $k(x)$.*

Proof. From the above it is clear that if $\beta = 0$ representatives for $\varphi_3(\alpha, \beta)$ can be chosen in $\mathbf{Q}(x)$. If $(\alpha, \beta) \in \mathscr{C}_{\mathbf{C}(x)}$ and $\beta \neq 0$ we may write $\alpha = \theta/\psi^2$, $\beta = \chi/\psi^3$ where θ, χ, ψ are in $\mathbf{C}[x]$ and θ and ψ are coprime. Let $\theta = fA^2$, $\theta - (a - 2b)\psi^2 = gB^2$, $\theta - (a + 2b)\psi^2 = hC^2$, where f, g, h are square-free polynomials. Then $fghA^2B^2C^2 = \chi^2$, so $fgh \in K^{*2}$, $\varphi_3(\alpha, \beta) = (fK^{*2}, gK^{*2}, hK^{*2})$. Since f, g, h are square-free and $fgh \in K^{*2}$, they have no common factor and we may write $f = f_1 f_2$, $g = f_1 j$, $h = f_2 j$ with $f_1, f_2, j \in C[x]$. Then $f_1 \mid (a - 2b), f_2 \mid (a + 2b)$, and $j \mid b$. So f_1, f_2, $j \in k[x]$.

2. POINTS OF INFINITE ORDER

$\mathscr{C}$ is not birationally equivalent to a curve over $\mathbf{C}$ unless $a = \lambda c^2$, $b = \mu c^2$ for some $\lambda, \mu \in \mathbf{C}$ and $c \in \mathbf{C}[x]$. Henceforth, we shall assume that this is not the case. Hence, by the function field analog of the Mordell–Weil theorem, [3], $\mathscr{C}_{\mathbf{C}(x)}$ is finitely generated. Each point of $\mathscr{C}_{\mathbf{C}(x)}$ is defined over some $K_0(x)$, where K_0 is a finite extension of $\mathbf{Q}$. Thus, there is a normal extension K_1/k, such that $\mathscr{C}_{\mathbf{C}(x)} = \mathscr{C}_{K_1(x)}$. Let $\Gamma = \mathrm{Gal}(K/k)$. Then Γ acts on $\mathscr{C}_{\mathbf{C}(x)}$. Γ also acts on the image of φ_3. But by Lemma 1 this action is trivial. Since φ_3 commutes with the actions of Γ we have proved the following lemma.

LEMMA 2. *Γ acts on $\mathscr{C}_{\mathbf{C}(x)}$ and the induced action on $\mathscr{C}/2\mathscr{C}$ is trivial.*

LEMMA 3. *Let Γ be a finite group and A a finitely generated torsion free abelian group on which Γ acts. If Γ induces the trivial action on $A/2A$ then there is a basis $\{a_i\}$ such that for all $\sigma \in \Gamma$, $\sigma a_i = \pm a_i$.*

Proof. Replacing Γ by a quotient group if necessary, we may assume that Γ acts faithfully on A.

(i) Let $a \in A$ and assume inductively on m that for all σ of odd order $a - \sigma a \in 2^m A$. (This is true for $m = 1$ and all a since Γ acts trivially on $A/2A$.) Let $\tau = \sigma^{(n+1)/2}$, where n is the order of σ. Then τ is of odd order and $\tau^2 = \sigma$. So by the inductive hypothesis $a - \tau a = 2^m b$ for some $b \in A$. $a - \sigma a = a - \tau a + \tau(a - \tau a) = 2^m(b + \tau b) = 2^{m+1}b + 2^m(b - \tau b)$ But $b - \tau b \in 2A$, so $a - \sigma a \in 2^{m+1}A$, which proves the inductive step. Therefore $a - \sigma a \in \bigcap_{m=1}^{\infty} 2^m A = \{0\}$. That is, $a = \sigma a$. Hence $\sigma = 1$ and Γ has no nontrivial elements of odd order.

(ii) If $\sigma \in \Gamma$ is of order 2, let $A_+ = \{a \mid \sigma a = a\}$ and $A_- = \{a \mid \sigma a = -a\}$. Let $a \in A$ $2a = (a + \sigma a) + (a - \sigma a) \in A_+ + A_-$. But $a - \sigma a \in 2A$, say $a - \sigma a = 2b$ Then $a + \sigma a = 2(b + \sigma a)$. Hence $\sigma(2b) = -2b$ and $\sigma(2(b + \sigma a)) = 2(b + \sigma a)$. Since A is torsion free, $b \in A_-$ and $(b + \sigma a) \in A_+$. Therefore $a = b + (b + \sigma a) \in A_- \oplus A_+$. So $A = A_- \oplus A_+$.

(iii) Suppose $\tau \in \Gamma$ is of order 4; $\sigma = \tau^2$ is of order 2, so A_- is non-empty. Let a be an element of A_- not divisible by 2, then $\tau a = a + 2c$ for some $c \in A$, and $\tau c = c + 2d$ for some $d \in A$.

$$-a = \sigma a = \tau^2 a = \tau a + 2\tau c = a + 4c + 4d, \qquad 2a = -4(c + d),$$

so $a = -2(c + d)$, contradicting our hypothesis. Thus there are no elements of order 4 in Γ.

(iv) Then Γ has exponent 2 and is therefore abelian. Now we prove the lemma by induction on n, the order of Γ. The lemma is trivial if $n = 1$. If $n > 1\Gamma$ has a subgroup G of index 2. Let $\sigma \notin G$ and A_+, A_- be as above. Since Γ is abelian, A_+ and A_- are invariant under G and so by the inductive hypothesis we can choose bases $\{a_i \mid 1 \leqslant i \leqslant s\}$ and $\{a_i \mid s + 1 \leqslant i \leqslant t\}$ of A_+ and A_-, respectively, so that for all $\tau \in G$ $\tau a_i = \pm a_i$. Then for all $\rho \in \Gamma$, $\rho = \sigma\tau$ with $\tau \in G$ and $\rho a_i = \pm a_i$. This completes the proof.

Let $\mathscr{F}$ be the group of points of finite order in $\mathscr{C}_{\mathbf{C}(x)}$ and $\Gamma = \mathrm{Gal}(K_1/k)$. Then we can apply Lemma 3 to $A = \mathscr{C}_{\mathbf{C}(x)}/\mathscr{F}$. Let $\{\mathfrak{a}_i \mid 1 \leqslant i \leqslant t\}$ be representatives in $\mathscr{C}_{\mathbf{C}(x)}$ of a basis of A such that $\sigma\mathfrak{a}_i = \pm\mathfrak{a}_i \bmod \mathscr{F}$, for all $\sigma \in \Gamma$. Let m be the order of $\mathscr{F}$. Then $\sigma(m\mathfrak{a}_i) = \pm m\mathfrak{a}_i$. Therefore $m\mathfrak{a}_i \in \mathscr{C}^{d_i}_{k(x)}$ where $k(d_i^{1/2})$ is the fixed field of $\{\sigma \in \Gamma \mid \sigma m\mathfrak{a}_i = m\mathfrak{a}_i\}$. We have now proved the following proposition.

PROPOSITION 2. *Let k be as in Lemma 1 and m be the order of $\mathscr{F}$. Then there are d_i, $1 \leqslant i \leqslant t$, in k^* such that $m\mathscr{C}_{\mathbf{C}(x)} \subseteq \mathscr{C}^{d_1}_{k(x)} \mathscr{C}^{d_2}_{k(x)}, \ldots, \mathscr{C}^{d_t}_{k(x)}$.*

COROLLARY. *If for all $d \in k^*$ the image of $\varphi_1 : \mathscr{C}^d_{k(x)} \to \mathbf{C}(x)^*/\mathbf{C}(x)^{*2}$ is the image of the points of order two and the image of $\varphi_2 : \mathscr{D}^d_{k(x)} \to \mathbf{C}(x)^*/\mathbf{C}(x)^{*2}$ is trivial, then there are no points of infinite order on $\mathscr{C}_{\mathbf{C}(x)}$ or $\mathscr{D}_{\mathbf{C}(x)}$.*

Proof. Let $\mathscr{C}_{\mathbf{C}(x)}$ be infinite. Then so is $\mathscr{C}^d_{k(x)}$ for some $d \in k^*$, by Proposition 2. We can choose $\mathfrak{a} \in \mathscr{C}^d_{k(x)}$ so that none of $\mathfrak{a}$, $\mathfrak{a} + \mathfrak{p}_0$, $\mathfrak{a} + \mathfrak{p}_+$, $\mathfrak{a} + \mathfrak{p}_-$ are divisible by two. Suppose $\mathrm{Im}(\varphi_1) = \{1, \varphi_1\mathfrak{p}_0, \varphi_1\mathfrak{p}_+, \varphi_1\mathfrak{p}_-\}$ and $\mathrm{Im}(\varphi_2) = \{1\}$, then one of $\mathfrak{a}$, $\mathfrak{a} + \mathfrak{p}_0$, $\mathfrak{a} + \mathfrak{p}_+$, $\mathfrak{a} + \mathfrak{p}_-$ is in $\ker \varphi_1$. Say $\mathfrak{a} \in \ker \varphi_1$. Then $\mathfrak{a} \in \mathrm{Im}(\theta_1)$, say $\mathfrak{a} = \theta_1\mathfrak{b}$ with $\mathfrak{b} \in \mathscr{D}^d_{k(x)}$. $\varphi_2\mathfrak{b} = 1$ so $\mathfrak{b} \in \mathrm{Im}(\theta_2)$, say $\mathfrak{b} = \theta_2\mathfrak{c}$ with $\mathfrak{c} \in \mathscr{C}^d_{k(x)}$. Then $\mathfrak{a} = \theta_1\theta_2\mathfrak{c} = 2\mathfrak{c}$, a contradiction that proves the corollary.

3. Points of Finite Order

We shall suppose that $a^2 - 4b^2$, $a + 2b$, $a - 2b$ are neither positive nor negative semidefinite. First, this implies that none of $\mathfrak{p}_0$, $\mathfrak{p}_+$, $\mathfrak{p}_-$ is special. Secondly $a^2 - 4b^2$, $a + 2b$, $a - 2b$ are not squares in $\mathbf{C}(x)$. Hence the points of order two on $\mathscr{C}$ are not in $\ker \varphi_1 = \mathrm{Im}(\theta_1)$ and thus not in the image of $\theta_1\theta_2$ (multiplication by 2). So there are no points of order 4 in $\mathscr{C}_{\mathbf{C}(x)}$. If $\mathfrak{a} = (\alpha, \beta)$ is a point of odd order, n, on $\mathscr{C}^{-1}_{\mathbf{R}(x)}$ then $\alpha \neq 0$. $\mathfrak{a} = 2[((n+1)/2)\,\mathfrak{a}] = \theta_1(\theta_2((n+1)/2)\,\mathfrak{a})$. So $\mathfrak{a}$ is in the image of $\theta_1 : \mathscr{D}^{-1}_{\mathbf{R}(x)} \to \mathscr{C}^{-1}_{\mathbf{R}(x)}$. Therefore $\varphi_1\mathfrak{a} = \mathbf{R}(x)^{*2}$, that is $-\alpha \in \mathbf{R}(x)^{*2}$. So α is not positive semidefinite and $\mathfrak{a}$ is not special.

Indeed Hellegouarch [2] has proved that a curve defined over $k[x]$ not birationally equivalent to one defined over k cannot have a point of prime order greater than three. A point of order three on $\mathscr{C}_{\mathbf{C}(x)}$ is of the form (α, β) where α is a root of $3\alpha^4 - 8a\alpha^3 + 6(a^2 - 4b^2)\,\alpha^2 + (a^2 - 4b^2)^2 = 0$ It is easy to check that for the curves we consider later there are no such points.

4. Valuations

In this section we describe some restrictions imposed by local considerations on a solution to the equation

$$dY^2 = X(X^2 - 2AX + C), \tag{4.1}$$

where $A, C \in k(x)$, and look in more detail at a particular example.

Let v be an additive valuation of $k(x)$, trivial on k. If $P = QR^2 + S$ with $P, Q, R, S \in k(x)$; P, Q, R nonzero and $v(S) > v(P)$, then we shall write $P \sim Q$. In other words P/Q is a square in the completion $(k(x))_v$ of $k(x)$ with respect to v. So $\sim$ is an equivalence relation.

Suppose the curve (4.1) has a point (α, β) defined over $k(x)$ with $\beta \neq 0$. We can write $\alpha = f\theta^2$ where f is a square-free polynomial in $k[x]$. Let $\gamma = \beta\theta\alpha^{-1}$ and $D = A^2 - C$. Then

$$df\gamma^2 = \alpha^2 - 2A\alpha + C \tag{4.2}$$

and

$$df\gamma^2 = (\alpha - A)^2 - D. \tag{4.3}$$

It is useful to discover when either α^2 or C has the smallest value of the terms on the right of (4.2). First, $v(\alpha^2)$ is the least value when $v(\alpha) < \min(v(A), 1/2\,v(C))$. Then $df \sim 1$. $v(C)$ is the least value when $v(\alpha) > \max(1/2v(C), v(C) - v(A))$. Then $df \sim C$. The following lemma is a reformulation of these conditions.

LEMMA 4. (i) *For valuations with* $v(A) \geqslant 1/2v(C)$ *either* $v(\alpha) = 1/2v(C)$ *or* $df \sim 1$ *or* $df \sim C$.

(ii) *For valuations with* $v(A) < 1/2v(C)$ *either* $v(A) \leqslant v(\alpha) \leqslant v(C) - v(A)$ *or* $df \sim 1$ *or* $df \sim C$.

We now take a particular example. Let $a = x(x + \mu)^3 - 1/2\nu^3 x$ $b = 1/4\nu^3 x$ where $\mu, \nu \in \mathbf{Q}$ and $\nu > \mu > 0$. Let ω be a cube root of unity and $k = \mathbf{Q}(\omega)$.

$$a - 2b = x(x + \mu - \nu)(x + \mu - \omega\nu)(x + \mu - \omega^2\nu) = x[(x + \mu)^3 - \nu^3]$$

$$a + 2b = x(x + \mu)^3$$

Thus $a^2 - 4b^2$ and b split into linear factors over k. If $x \geqslant \nu - \mu$ or $x \leqslant -\mu$ then $a(x) > 0$ and if $-\mu < x < \nu - \mu$ then $(a^2 - 4b^2) < 0$. So $F(x, y) = 1 + ay^2 + b^2y^4$ is positive definite as in section 1. Also all of the assumptions of Sections 2 and 3 hold.

Let $A = a$, $C = a^2 - 4b^2$, $D = 4b^2$. Then the curve $\mathscr{C}^d$ is given by (4.1). Suppose $\mathfrak{a} = (\alpha, \beta)$ is a point on $\mathscr{C}^d_{k(x)}$ with $\varphi_1\mathfrak{a} = f\mathbf{C}(x)^{*2} \neq \mathbf{C}(x)^{*2}$.

First, take v to be any valuation with $v(C) = 0$. Now $v(A) \geqslant 0$. By Lemma 4(i) either $v(\alpha) = 0$ or $df \sim$ something with value 0, so in either case $v(f)$ is even. Since f is a square-free polynomial $v(f) = 0$. Hence $f \mid x(x + \mu)(x + \mu - \nu)(x + \mu - \omega\nu)(x + \mu - \omega^2\nu)$.

Second, take v to be v_∞, the degree valuation. $v(A) = -4$, $v(C) = -8$ and by Lemma 4(i) $v(f)$ is even, that is the degree of f is even.

$\varphi_1(\mathfrak{p}_+) = x(x + \mu)\,\mathbf{C}(x)^{*2}$, so replacing $\mathfrak{a}$ by $\mathfrak{a} + \mathfrak{p}_+$, if necessary, we may suppose that $x \nmid f$. Further, $\varphi_1(\mathfrak{p}_0) = (x + \mu)[(x + \mu)^3 - \nu^3]\,\mathbf{C}(x)^{*2}$ so by also adding $\mathfrak{p}_0$ if necessary, we may suppose that $(x + \mu) \nmid f$. Therefore $f = e(x - \chi_2)(x - \chi_3)$ where $e \in k^*$ and e is unique upto multiplication by a square in k^*, and χ_1, χ_2, χ_3 is some permutation of $\nu - \mu, \omega\nu - \mu, \omega^2\nu - \mu$.

Again let $v = v_\infty$. Now $C \sim 1$ and $f \sim e$, so by Lemma 4(i) either $de \in k^{*2}$ or $v(\alpha) = 1/2\, v(C) = -4$. Suppose $v(\alpha) = -4$, then $v(D) = -2$ and, unless $\alpha \sim A$, $v(\alpha - A) = -4$. Then from (4.3) $df \sim (\alpha - A)^2 \sim 1$. Therefore if $v(\alpha) = -4$ either $\alpha \sim A$ or $de \in k^{*2}$. Since $A \sim 1$ and $\alpha \sim e$ we have the following:

$$\text{either } e \text{ or } de \in k^{*2}. \tag{4.4}$$

Next, let $v = v_0$, the valuation corresponding to the polynomial x. $v(A) = 1$, $v(C) = 2$, and $v(\alpha)$ is even. By Lemma 4(i) $df \sim 1$ or $df \sim C$. But $C \sim \mu^3(\mu^3 - \nu^3) = -\mu^3\chi_1\chi_2\chi_3$ and $f \sim e\chi_2\chi_3$. Therefore

$$\text{either } de\chi_2\chi_3 \text{ or } -de\mu\chi_1 \in k^{*2} \tag{4.5}$$

Putting (4.4) and (4.5) together, we have either

(i) $\chi_2\chi_3 \in k^{*2}$ or $-\mu\chi_1 \in k^{*2}$; or

(ii) $e \in k^{*2}$ and $d \in \chi_2\chi_3 k^{*2}$ or $d \in -\mu\chi_1 k^{*2}$.

We shall later choose μ, ν so that (i) does not hold. So suppose (ii) holds. We may take $e = 1$.

Let $v = v_{\chi_2}$, the valuation corresponding to $(x - \chi_2)$. $v(A) = 0$, $v(C) = 1$, $v(f) = 1$ so $v(\alpha)$ is odd. By Lemma 4(ii) $df \sim 1$ or $df \sim C$ or $v(\alpha) = 1$. The first of these cannot hold since $v(f) = 1$. The second is equivalent to $d(\chi_2 - \chi_3) \in (\chi_2 + \mu)(\chi_2 - \chi_1)(\chi_2 - \chi_3)\, k^{*2}$, that is

$$d \in \nu(\chi_2 - \chi_1)\, k^{*2} \tag{4.6}$$

since $\chi_2 + \mu = \omega^i\nu$ and $\mathbf{C} \in k^{*2}$.

Finally if $v(\alpha) = 1$ then $v(\theta) = 0$. Dividing (4.2) by f we get

$$d\gamma^2 = f\theta^4 - 2A\theta^2 + x^2(x + \mu)^3 (x - \chi_1) \tag{4.7}$$

$A = (a - 2b) + 2b$ and $(x - \chi_2) | a - 2b$. Therefore $A(\chi_2) = 1/2\nu^3\chi_2 (\chi_2 + \mu)^3 = (\omega^i\nu)^3 = \nu^3$. Evaluating (4.7) at $x = \chi_2$ we get

$$d[\gamma(\chi_2)]^2 = -\nu^3\chi_2[\theta(\chi_2)]^2 + \chi_2{}^2\nu^3(\chi_2 - \chi_1).$$

That is $dS^2 + \nu\chi_2 T^2$ represents $\nu(\chi_2 - \chi_1)$. Notice that if (4.6) holds then $dS^2 + \nu\chi_2 T^2$ represents $\nu(\chi_2 - \chi_1)$ with $T = 0$. To sum up we have proved the following lemma.

LEMMA 5. *If there is a point* $\mathfrak{a}$, *not of order two, on* $\mathscr{C}^d_{k(x)}$ *for some* $d \in k^*$, *with* $\varphi_1(\mathfrak{a}) \neq \mathbf{C}(x)^{*2}$ *then either*

(i) $\chi_2\chi_3 \in k^{*2}$ *or* $-\mu\chi_1 \in k^{*2}$; *or*

(ii) *one of*

$$\chi_2\chi_3 S^2 + \nu\chi_2 T^2, \tag{4.8}$$

and

$$-\mu\chi_1 S^2 + \nu\chi_2 T^2 \tag{4.9}$$

represents $\nu(\chi_2 - \chi_1)$ *over* k.

In fact these are conditions for

$$edY^2 = e^2(x - \chi_2)(x - \chi_3)\, X^4 - 2eAX^2 + x^2(x + \mu)^3 (x - \chi_1)$$

to have points in the various completions of $k(x)$ we have considered.

The main battle is over. Now we must look at the rather easier case of the curve $\mathscr{D}^d_{k(x)}$. Put $A = -2a$, $C = 16b^2$, $D = 4(a^2 - 4b^2)$. Then the curve $\mathscr{D}^d$ is given by (4.1). Suppose $\mathfrak{a} = (\alpha, \beta)$ is a point on $\mathscr{D}^d_{k(x)}$ with $\varphi_2(\mathfrak{a}) \neq \mathbf{C}(x)^{*2}$. As before we can deduce that $f \mid C$ so $f \mid x$. Therefore we may write $f = ex$ with $e \in k^*$. Let $v = v_{x_2}$. Then $v(A) = v(C) = 0, v(D) = 1$ and $C \sim 1$. By Lemma 4(i), $v(\alpha) = 0$ or $df \sim 1$. If $v(\alpha) = 0$ then $v(\alpha - A)^2 = 0$ or $v(\alpha - A)^2 > v(D)$. The second case is impossible for then the right-hand side of (4.3) would have value 1 and the left-hand side even value. So $df\gamma^2 \sim (\alpha - A)^2$, that is, $df \sim 1$. Thus in all cases $df \sim 1$. In other words $de\chi_2 \in k^{*2}$. Similarly $de\chi_3 \in k^{*2}$ and so $\chi_2\chi_3 \in k^{*2}$.

LEMMA 6. *If there is a point* $\mathfrak{a}$ *on* $\mathscr{D}^d_{k(x)}$ *for some* $d \in k^*$ *with* $\varphi_2(\mathfrak{a}) \neq \mathbf{C}(x)^{*2}$, *then* $\chi_2\chi_3 \in k^{*2}$.

5. SQUARES IN $\mathbf{Q}(\omega)$

We find in this section some sufficient conditions on μ, ν for the requirements of Lemmas 5 and 6 to fail. There are many alternative choices of a congruence condition on μ and ν such that neither (4.8) nor (4.9) represents $\nu(\chi_2 - \chi_1)$. We have chosen the easiest to prove.

LEMMA 7. *Let* $\nu > \mu > 0$ *and* χ_1, χ_2, χ_3 *be a permutation of* $\nu - \mu$, $\omega\nu - \mu$, $\omega^2\nu - \mu$. *If* $\nu^2 - \nu\mu + \mu^2 \notin \mathbf{Q}^{*2}$ *and* $3(\nu - \mu)\mu \notin \mathbf{Q}^{*2}$ *then* $\chi_2\chi_3 \notin k^{*2}$ *and* $-\mu\chi_1 \notin k^{*2}$.

Proof. If $a \in \mathbf{Q} \cap k^{*2}$ then $a \in \mathbf{Q}^{*2}$ or $-3a \in \mathbf{Q}^{*2}$. If $a \in k^{*2} \backslash \mathbf{Q}$ then $\mathrm{Norm}_{k/\mathbf{Q}}(a) \in \mathbf{Q}^{*2}$. $-\mu\chi_1 = -\mu(\nu - \mu)$ or $-\mu(\omega\nu - \mu)$ or its conjugate. Further, since none of $-\mu(\nu - \mu)$, $3\mu(\nu - \mu)$, $\mu^2(\nu^2 - \nu\mu + \mu^2)$ are in $\mathbf{Q}^{*2}$, $-\mu\chi_1 \notin k^{*2}$. Similarly $\chi_2\chi_3 = (\nu - \mu)(\omega\nu - \mu)$ or its conjugate, or $\nu^2 - \nu\mu + \mu^2$ and since $-3(\nu^2 - \nu\mu + \mu^2)$ is negative, $\chi_2\chi_3 \notin k^{*2}$.

LEMMA 8. *If* $\mu, \nu \in \mathbf{Z}$, $\mu = (-3)^n \lambda$, *where* $3 \nmid \lambda$, $n \geqslant 1$, $\lambda \equiv -\nu \pmod 3$, *then neither* (4.8) *nor* (4.9) *represents* $\nu(\chi_2 - \chi_1)$ *over* k.

Proof. Let $\pi = (-3)^{1/2}$, then $\chi_1 \equiv \chi_2 \equiv \chi_3 \equiv \nu \pmod \pi$. So $\pi \mid \nu(\chi_2 - \chi_1)$, but $\pi^2 \nmid \nu(\chi_2 - \chi_1)$. Suppose (4.8) represents $\nu(\chi_2 - \chi_1)$. Then $\pi \nmid S$ and $\pi \nmid T$, so $\chi_2\chi_3 + \nu\chi_2(T/S)^2 \equiv 0 \pmod \pi$. Thus -1 is a square mod π; a contradiction. In (4.9) replace S by $S\pi^{-n}$ to obtain $-\lambda\chi_1 S^2 + \nu\chi_2 T^2$. By the same argument as before, this cannot represent $\nu(\chi_2 - \chi_1)$.

6. Conclusions

Putting together Lemmas 5–8, and the corollary to the proposition we deduce

THEOREM. *Let* μ, ν *be integers with* $0 < \mu < \nu$, $3 \mid \mu$, $\mu = (-3)^n\lambda$, $3 \nmid \lambda$, $\lambda \equiv -\nu \pmod 3$, *and* $3\mu(\nu - \mu)$ *and* $\nu^2 - \nu\mu + \mu^2$ *not integer squares. Then the curve*

$$Y^2 = X(X - x(x + \mu)^3)(X - x(x + \mu)^3 + \nu^3 x) \tag{6.1}$$

has no points of infinite order defined over $\mathbf{C}(x)$.

By the remark at the end of Section 3, we can see that (6.1) has no points, other than those of order two, defined over $\mathbf{C}(x)$.

COROLLARY. *With the above conditions*

$$F(x, y) = x(x + \mu)^3 y^2 + (1 + 1/4\nu^3 xy^2)^2$$

is a positive definite form and is not the sum of three squares in $\mathbf{R}(x, y)$.

A small numerical example is given by $\mu = 3$, $\nu = 10$,

$$F(x, y) = x(x + 3)^3 y^2 + (1 + 250xy^2)^2.$$

Acknowledgment

I should like to thank Professor Cassels for suggesting this problem to me.

References

1. J. W. S. Cassels, W. J. Ellison, and A. Pfister, On sums of squares and on elliptic curves over function fields, *J. Number Theory* **3** (1971), 125–149.
2. Y. Hellegouarch, Étude des points d'ordre fini des variétés abéliennes de dimension un définies sur un anneau principal, *J. Reine Angew. Math.* **244** (1970), 20–36.
3. S. Lang, "Diophantine Geometry," Interscience, New York, 1962.
4. A. Pfister, Zur Darstellung definiter Funktionen als Summe von Quadraten, *Invent. Math.* **4** (1967), 229–237.